REMARKS

I. CLAIM STATUS

In the above-identified patent application, claims 1-10 and 12-32 are currently pending, of which claims 1, 22, and 29-32 are independent claims. No amendments to the claims are made herewith. All of the outstanding claim rejections are traversed for the reasons set out below.

II. THE CLAIM REJECTIONS UNDER 35 U.S.C. § 103(a) SHOULD BE WITHDRAWN

The September 2, 2009 Office Action contained multiple rejections under 35 U.S.C. § 103(a), namely:

- a rejection of claims 1-2, 5-9, 12-19, 22-26, and 29-32[1] as being unpatentable for obviousness over Saito et al. "Privacy Enhanced Access Control by SPKI" (hereinafter "Saito") in view of U.S. Patent No, 5,717,758 to Micall (hereinafter "Micall");
- a rejection of claims 3-4, 10, 20-21, and 27-28[2] as being unpatentable for obviousness over Saito in view of Micall, and further in view of U.S. Patent Application Publication No. 2007/0189542 to Alldredge (hereinafter "Alldredge").

Such rejections are traversed.

In the September 2, 2009 Office Action, the examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data" (September 2, 2009 Office Action, page 24, but alleged that it would be obvious to combine Micall with Saito to yield the subject matter of Applicants' independent claims. As detailed below, Saito relates to Simple Public Key Infrastructure (SPKI), while Micall relates to Public Key Infrastructure ("PKI"), such that Micall is not properly combinable with Saito to support the rejection of any of Applicants' independent claims. The

[1] See September 2, 2009 Office Action, pp. 3-11.
[2] See September 2, 2009 Office Action, pp. 11-12.

distinctions between PKI and SPKI are discussed below to provide appropriate background for the impropriety of combining the disclosures of Micall and Saito.

A. Discussion of Public Key Infrastructure (PKI) and Simple Public Key Infrastructure (SPKI)

It is generally understood in the art that both Public Key Infrastructure ("PKI") and Simple Public Key Infrastructure ("SPKI") represent different authentication solutions, with PKI utilizing a certificate authority (CA) that binds public keys with user identities, but with SPKI eliminating the need for any certificate authority by use of an authorization loop (whereby the verifier is also the issuer (such that public authentication of public key information, and use of a certificate authority, is *unnecessary*). See, e.g., the following excerpts:

> SPKI/SDSI (Simple Public Key Infrastructure/Simple Distributed Security Infrastructure): The SPKI efforts of the IETF have been combined with SDSI, an approach outlined by MIT's Ron Rivest and Microsoft's Butler Lampson. ... **SDSI/SPKI differs from the more developed and accepted PKIX (Public Key Infrastructure X.509) in specifying a highly distributed, client-focused trust model** relying on delegated human-readable certificates. For example, a business might issue "salesperson" certificates to employees and those employees might issue "salesperson-customer" certificates to customers, and only those customers identified as customers associated with a salesperson will gain entry. SDSI/SPKI also is more flexible than PKIX in letting end users define rules for processing certificates. It also rejects the complex ASN.1 syntax of X.509. **Considerable control is put in the hands of end users, rather than relying on a centralized infrastructure for establishing identities**. The infrastructure also puts an emphasis on short-lived, ephemeral certificates, reissued daily, for example, in lieu of extensive reliance on CRLs.

Source: Network Computing "Certificate Authority Glossary," available online at http://www.networkcomputing.com/813/813f2glos.html (emphasis added).

See also Clarke, "SPKI/SDSI HTTP Server / Certificate Chain Discovery in SPKI/SDSI," Thesis Submitted to Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Sept. 2001, page 81, table 3.1, (available online at http://groups.csail.mit.edu/cis/theses/clarke-masters.pdf) as reproduced below.

X.509	Name Space:	Global
	Types of Certificates:	Name Certificates
	Name-to-Key binding:	Single-valued function: each global name is bound to exactly one key (assuming each user has a single public-private key pair).
	CA Characteristics:	Global Hierarchy. There are commercial X.509 CAs. X.509 communities are built from the top-down.
	Trust Model:	Hierarchical Trust Model. Trust originates from a 'trusted' CA, over which the guardian may or may not have control. A requestor provides a *chain of authentication* from the 'trusted' CA to the requestor's key.
	Signatures:	Each certificate has one signature, belonging to the issuer of the certificate.
	Certificate Revocation:	Uses CRLs
PGP	Name Space:	Global
	Types of Certificates:	Name Certificates
	Name-to-Key binding:	Single-valued function: each global name is bound to exactly one key (assuming each user has a single public-private key pair).
	CA Characteristics:	Egalitarian design. Each key can issue certificates. PGP communities are built from the bottom-up in a distributed manner.
	Trust Model:	*Web of Trust*
	Signatures:	Each certificate can have multiple signatures; the first signature belongs to the issuer of the certificate.
	Certificate Revocation:	A suicide note is posted on PGP certificate servers, and widely distributed to people who have the compromised key on their public keyrings.
SPKI/SDSI	Name Space:	Local
	Types of Certificates:	Name Certificates, Authorization Certificates
	Name-to-Key binding:	Multi-valued function: each local name is bound to zero, one or more keys (assuming each user has a single public-private key pair).
	CA Characteristics:	Egalitarian design. The principals are the public keys. Each key can issue certificates. SPKI/SDSI communities are built from the bottom-up in a distributed manner.
	Trust Model:	Trust originates from the guardian. A requestor provides a *chain of authorization* from the guardian to the requestor's key. The infrastructure has a clean, scalable model for defining groups and delegating authority.
	Signatures:	Each certificate has one signature, belonging to the issuer of the certificate.
	Certificate Revocation:	Advocates using short validity periods and *Certificates of Health*.

Table 3.1: Comparison of X.509, PGP, and SPKI/SDSI

The foregoing table summarizes stark differences between PKI ("X.509") and SPKI with respect to Certificate Authority (CA) Characteristics and Trust Model. As indicated above, PKI (X.509) employs a Certificate Authority having a "global hierarchy" with commercial certificate authorities and communities that are built from the top down. In contrast, a SPKI structure is characterized by an "egalitarian design" wherein the principals are the public keys and each key can issue certificates, with SPKI communities being built from the bottom-up in a distributed manner. The trust model used by PKI (X.509) is a hierarchical trust model with trust originating from the Certificate Authority (CA), and with a requestor providing a chain of authenticity from the 'trusted' CA to the requestor's key. In contrast, SPKI utilizes a trust model in which trust originates from the guardian. A requestor provides a chain of authorization from the guardian to the requestor's key. As a result, SPKI has no need for a commercial CA.

It is noted that Wikipedia also provides a discussion of Public Key Infrastructure and Simple Public Key Infrastructure that is consistent with the foregoing references[3,4,5].

B. Law Regarding Obviousness

To support a rejection under 35 U.S.C. 103, **the prior art reference(s) must teach all of the limitations of the claims.** MPEP § 2143.03.

---

[3] "A Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. A PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA. The term trusted third party (TTP) may also be used for certificate authority (CA)." (*See* http://en.wikipedia.org/wiki/Public_key_infrastructure.)

[4] "An alternative approach to the problem of public authentication of public key information ... which however does not deal with public authentication of public key information, is the simple public key infrastructure ("SPKI") that grew out of 3 independent efforts to overcome the complexities of X.509 and PGP's web of trust. SPKI does not bind people to keys, as the key is what is trusted, rather than the person. SPKI does not use any notion of trust, as the verifier is also the issuer. This is called an "authorization loop" in SPKI terminology, where authorization is integral to its design." (*See* http://en.wikipedia.org/wiki/Public_key_infrastructure.)

[5] SPKI specification defines an authorization certificate format, providing for the delineation of privileges, rights or other such attributes (called authorizations) and binding them to a public key. [SPKI] does not define a role for a commercial Certificate Authority (CA). In fact, **one premise behind SPKI is that a commercial CA serves no useful purpose.** (*See* http://en.wikipedia.org/wiki/Simple_public_key_infrastructure.)

In considering a reference for its effect on patentability, the reference is required to be considered in its entirety, including portions that **teach away** from the invention under consideration. Simply stated, the prior art must be considered as a whole. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984) (emphasis added); MPEP § 2141.02. "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *Application of Wesslau*, 353 F.2d 238, 241 (C.C.P.A. 1965); *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve*, 796 F.2d 443, 448 (Fed. Cir. 1986), cert. denied, 484 U.S. 823 (1987). The Federal Circuit and its predecessor court have repeatedly held that **if references taken in combination would produce a 'seemingly inoperative' device, then such references teach away from the combination** and cannot serve as predicates for a *prima facie* case of obviousness. *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 60 USPQ2d 1001, 1010 (Fed. Cir. 2001); *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 52 USPQ2d 1294, 1298 (Fed. Cir. 1999) (proposed combination of references that would be inoperable for intended purpose supports teaching away from combination); *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) (inoperable modification teaches away); *In re Sponnoble*, 405 F.2d 578, 587, 160 USPQ 237, 244 (C.C.P.A. 1969) (references teach away from combination if combination produces seemingly inoperative device).

According to the U.S. Supreme Court decision in *KSR International Co. v. Teleflex Inc.*, 127 S.Ct 1727, 167 L.Ed.2d 705, 82 USPQ2d 1385 (2007), the court did not disavow the previous "teaching, motivation or suggestion" or "TSM" test, but stated that such TSM text *should not be strictly applied* in determining obviousness. In connection with this point, the Supreme Court stated that:

> "A patent composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art. … [Rather], it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant art to combine the [prior art] elements in the manner claimed." *KSR*, 82 USPQ2d at 1389.

It is fundamental to a proper rejection of claims under 35 U.S.C. § 103 that an examiner must present a convincing line of reasoning supporting the rejection. MPEP 2144 ("Sources of Rationale Supporting a Rejection Under 35 U.S.C. 103"), citing *Ex parte Clapp*, 227 USPQ 972 (Bd. Pat. App. & Inter. 1985). The Supreme Court in *KSR* affirmed the validity of such approach, stating that "**there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness**." *KSR*, 82 USPQ2d at 1396.

In *KSR*, the Supreme Court further confirmed that **references that teach away from the invention are evidence of the non-obviousness** of a claimed invention, (*KSR*, 82 USPQ2d at 1395, 1399) and reaffirmed the principle that a factfinder judging patentability "should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning."

Following *KSR*, the Federal Circuit held that although "rigid" application of the "teaching, suggestion, or motivation" ("TSM") test for obviousness is improper, **application of a flexible TSM test remains the primary guarantee against improper "hindsight" analysis**, because a flexibly applied TSM test ensures that the obviousness analysis proceeds on the basis of evidence in existence before time the application was filed, as required by 35 U.S.C. §103. *Ortho-McNeil Pharm. Inc. v. Mylan Labs., Inc.*, 520 F3d 1358, 86 USPQ2d 1196, 1201-02 (Fed. Cir. 2008).

A suggestion to combine references **cannot require substantial reconstruction or redesign** of such references, **or a change in basic operating principles** of a construction of a reference, to arrive at the claimed invention. *In re Ratti*, 270 F.2d 810, 123 USPQ 349, 352 (C.C.P.A. 1959). *See also* MPEP 2143.01 ("If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious.')

C. No Basis Exists for the Hypothetical Combination of Saito and Micall

Saito is directed to a privacy enhanced service scheme utilizing Simple Public Key Infrastructure (SPKI). Saito describes his privacy-enhanced access control system

provides the useful property of being "light and efficien[t]," specifically stating the following:

> "Since public key is **not mapped to ID** in an SPKI certificate, public key can be generated for a service or a set of services and discarded after its usage or lifetime. This **disposable** key scheme alleviates the management of public keys."

(Saito, pg. 302, second column.)

Saito describes another useful property of his privacy-enhanced access control system as being "self-verifiable," specifically stating the following:

> "In the SPKI scheme, there is a chain of verification: **without a server's or third party's help, clients can verify certificates by themselves**."

(Saito, pg. 302, second column.)

Saito therefore extols the benefits of a SPKI system as including verification of certificates without help of a server or third party.

In the September 2, 2009 Office Action at page 4, the examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data." Thereafter, the examined indicated that "Micall discloses reissuing valid certificates" and proposed combining this feature of Micall with Saito's disclosure. (September 2, 2009 Office Action, page 4).

In contrast to the SPKI-based system of Saito, Micall is directed to a traditional PKI-based system involving a certificate authority (CA), wherein an intermediary (a "witness") processes authenticated certificate information to construct authenticated deduced information. Such a witness system enables users to save transmission costs of certificate information (e.g., reducing need to transmit a long Certificate Revocation List (CRL), or search the CRL, to establish whether a given certificate has been revoked). An advantage of a witness system according to Micall is that, in comparison to direct communication with a CA, the intermediary provides much shorter answers when authenticating the status of issued certificates. (Micall, col. 8, lines 38-45.)

The proposed combination of Micall and Saito to yield Applicants' invention is not proper for at least the first reason that such a combination would change the principle

of operation of the art being modified. It is well settled that a suggestion to combine references supporting an obviousness rejection under 35 U.S.C. 103 cannot require substantial reconstruction or redesign of such references, or a change in basic operating principles of a construction of a reference, to arrive at the claimed invention. See *In re Ratti, supra,* and MPEP 2143.01. Saito discloses a SPKI system specifically designed to permit clients to verify certificates by themselves **without use** of a server or third party. In contradistinction to Saito, Micall discloses a PKI system that **requires use** of a certificate authority, in conjunction with a witness (intermediary). The proposed modification of Saito to include an infrastructure using a third party to verify certificates (according to Micall) would contradict a primary operating principle of Saito to permit clients to verify certificates without help of a server or third party. Moreover, the proposed combination of Micall and Saito would produce a "seemingly inoperative" system, which would teach away from the hypothetical combination and cannot serve as a predicate for a *prima facie* case of obviousness[6].

In the September 2, 2009 Office Action at page 2, the examiner stated that "though Micall requires a Certificate Authority, and Saito does not require help from a server or third party, if Saito used an infrastructure which used a third party, this would not destroy the system of Saito." Applicants disagree with the examiner's characterization in this regard as not based in fact or applying the proper legal standards relevant to an obviousness rejection under 35 U.S.C. 103. Applicants are not aware of any applicable legal standard articulating unconditional "destruction" of a system as a threshold for teaching away from obviousness. Repeating a first legal standard articulated above, a suggestion to combine references supporting an obviousness rejection "cannot require substantial reconstruction or redesign of such references, or a change in basic operating principles of a construction of a reference, to arrive at the claimed invention." Since the examiner does not dispute that Micall requires a

[6] See *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 60 USPQ2d 1001, 1010 (Fed. Cir. 2001); *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 52 USPQ2d 1294, 1298 (Fed. Cir. 1999) (proposed combination of references that would be inoperable for intended purpose supports teaching away from combination); *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) (inoperable modification teaches away); *In re Sponnoble*, 405 F.2d 578, 587, 160 USPQ 237, 244 (C.C.P.A. 1969) (references teach away from combination if combination produces seemingly inoperative device

Certificate Authority, and that Saito specifically avoids use of an intermediary[7], it is clear that the proposed modification of Saito to require usage of a Certificate Authority would entail substantial reconstruction or redesign, or a change in basic operating principles. Repeating a second legal standard articulated above, a proposed combination of references that would produce a "seemingly inoperative" system teaches away from the hypothetical combination and cannot support a *prima facie* case of obviousness. Given the divergent basic operating principles of Micall and Saito (i.e., with one requiring use of a certificate authority and the other specifically avoiding a certificate authority), there is no indication that the PKI-based system of Micall would be compatible with the SPKI-based system of Saito to produce an operative combined system. The hypothetical combination of references would therefore be "seemingly inoperative" for its intended purpose. Accordingly, the proposed combination of Micall and Saito is not supportable.

Moreover, to support the hypothetical combination of Micall and Saito, the examiner stated:

> "It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure [of Saito] to include reissuing valid SPKI certificates such as that taught by Micall **in order [to] reduce processing overhead by reissuing valid certificate instead of generating a new certificate**."

(September 2, 2009 Office Action, page 4). The foregoing rationale advanced by the examiner for combining Micall and Saito does not constitute "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" as required by *KSR, supra*. Saito specifically characterizes his SPKI system as being advantageous because it utilizes a disposable key scheme that alleviates the management of public keys (See Saito, pg. 302, second column.) This **directly contradicts the examiner's assertion that one skilled in the art would combine Micall with Saito to reduce processing overhead**, since addition of Micall's PKI-based complex key management system (i.e., requiring a Certificate Authority) as proposed by the examiner **would increase processing overhead**. The obviousness rejections premised on the hypothetical combination of Saito and Micall are erroneous for at least the reason that the examiner

[7] September 2, 2009 Office Action, page 2.

has failed to consider portions of Saito that teach away from the combination[8]. Given such teaching away, the examiner's rationale supporting the hypothetical combination of references does not embody "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness," as required by the Supreme Court in *KSR, supra.*

Each of claims 1, 22, 29, 30, 31, and 32 is allowable over Saito for at least the reason that Saito fails to disclose the feature of "wherein the concealing data remains fixed for reissued associations." Since the rejections of Applicants' independent claims 1, 22, 29, 30, 31, and 32 under 35 U.S.C. 103 are all premised on the hypothetical combination of Micall and Saito, and it has been demonstrated that such hypothetical combination of Micall and Saito is not supportable, no basis remains for maintaining such claim rejections.

Alldredge has been cited by the exasminer as disclosing "a method for secured electronic commerce using sequences of one time pads for concealing transmitted messages" and "a cryptographic system that includes a secret security identifier ... with a message and encrypts a the message containing the secret security identifier using secret domain key[9]. Alldredge fails to remedy the above-identified lack of support for combining Micall and Saito, or to remedy the deficiencies of Saito in disclosing all elements of Applicants' independent claims 1, 22, 29, 30, 31, and 32.

Accordingly, withdrawal of the rejections of Applicants' independent claims 1, 22, 29, 30, 31, and 32 is warranted, and is respectfully requested. Since dependent claims inherently include all of the features of the claims on which they depend[10], all claims depending (whether directly or indirectly) from independent claims 1, 22, 29, 30, 31, and 32 are likewise patentably distinguished over the cited art. Applicants respectfully submit that all pending claims are in form and condition for allowance.

---

[8] See., e.g., *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984) (emphasis added); MPEP § 2141.02.
[9] September 2, 2009 Office Action, page 12.
[10] 35 U.S.C. 112, fourth paragraph.

CONCLUSION

In light of the foregoing, Applicants respectfully submit that all of the now-pending presented claims are in condition for allowance. Examination of the enclosed claims and issuance of a notice of allowance are earnestly solicited. Should any issues remain that may be amenable to telephonic resolution, the examiner is invited to telephone the undersigned attorneys to resolve such issues as expeditiously as possible.

In the event there are any errors with respect to the fees for this response or any other papers related to this response, the Director is hereby given permission to charge any shortages and credit any overcharges of any fees required for this submission to Deposit Account No. 14-1270.

Respectfully submitted,

By: /vincent k. gustafson/
Vincent K. Gustafson
Registration No.: 46,182

INTELLECTUAL PROPERTY/
TECHNOLOGY LAW
P.O. Box 14329
Research Triangle Park, NC 27709
Phone: 919-419-9350

Dated: December 2, 2009

For: Kevin C. Ecker
Registration No.: 43,600
Phone: (914) 333-9618

Please direct all correspondence to:
Kevin C. Ecker, Esq.
Philips Intellectual Property & Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001